UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/846,103	04/30/2001	Dmitry O. Gryaznov	002.0160.01	5029

22895 7590 03/11/2005

PATRICK J S INOUYE P S
810 3RD AVENUE
SUITE 258
SEATTLE, WA 98104

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/846,103	GRYAZNOV ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 December 2004* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 April 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☒ Interview Summary (PTO-413) Paper No(s). *2/25/05* .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 12/10/2004, applicant has amended claims 1, 3, 4, 17, 19, 20, 34, 35, 39, and 40. The following claims 1-44 are presented for examination.

2. The amendments to the specification, pages 2-3, filed on 12/10/2004 have been considered and the objection has been withdrawn. The objection to the drawings has been withdrawn with respect to the amended specifications. The 35 USC 112 rejection to claims 4, 20, 35, and 40 has been withdrawn with respect to the amended claims.

3. Applicant's arguments, pages 2-3, filed on 12/10/2004, with respect to the rejection of claims 1-44 have been fully considered, and they are persuasive as amended. However, the claims contain subject matter, which are not disclosed in the disclosure as claimed (see below). Chen et al (5,951,698) does not explicitly teach "traversing the hierarchical parse tree toe retrieve each suspect string" Upon further consideration, claims 1-44 are rejected on a new ground of rejection in view of Chen et al (5,960,170) under 35 USC 103(a). The rejection of the dependent claims not challenged by applicant still applies in this office action.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to

enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1, 17, 33, 34, 39, and 44 and the intervening claims are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. "a macro virus checker traversing the hierarchical parse tree to retrieve each suspect string" is not supported by the disclosure. The disclosure on page 7, line 19 through page 8, line 18 describes: checking macro virus families based on a suspect string and page 11, lines 4-25) describes a token from the parse tree being compared with the string for matching. Also each data file defining macro virus attributes ...for known macro viruses that are each comprised of at least one macro" is not found where it is supported in the specification.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to

which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.1 **Claims 1-44** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,951,698 to **Chen et al** in view of US Patent 5,960,170 to **Chen et al** hereafter **Chen**.

5.2 **As per claims 1, 17, 33, 34, 39, and 44, Chen et al.** substantially discloses a method and system for identifying a macro virus family using a macro virus definitions database, comprising: a virus information module that provides comparison data that includes set of identifiers strings of data and signatures for identifying known viruses (column 7, lines 47-57 and column 8, lines 58-67) that meets the recitation of maintaining a macro virus definitions database comprising a set of indices and macro virus definition data files with each index referencing one or more of the macro virus definition data files and each macro virus definition data file defining macro virus attributes for known macro viruses that are comprised of at least one macro; **Chen et al** discloses using file types for associating macro so that macros can be located and suggests to configure the scanning module to detect only certain classes that meets the recitation of organizing the sets of the indices and the macro virus definition data files into a hierarchy according to macro virus families based on a type of application to which the macro applies, for example (see column 14, line 52 through column 15); comparing a suspect string to the macro virus attributes defined in the one or more macro virus definition data files for each macro virus family in the macro virus definitions database, for example (see column 14, line 52 through column 15); and determining each macro virus family to which the suspect string belongs from

the index for each macro virus definition data file at least partially containing the suspect string or file, for example (see column 13, line 20 through column 14 and column 14, line 52 through column 15). **Chen et al** does not explicitly disclose using a hierarchical parse tree to retrieve each suspect string, which is also well known. **Chen** in an analogous art discloses organizing the sets of the indices and the macro virus definition data files into a hierarchy according to macro virus families based on a type of application to which the macro applies (column 18, lines 16-27 and column 19, lines 15-30 *(US Patent 5,960,170)*) and parsing a suspect file into tokens comprising one of individual string constants and source code text and storing the tokens as suspect strings into specific directories that meets the recitation of a hierarchical parse tree and traversing the hierarchical parse tree to retrieve each suspect string for comparison (column 19, lines 15-37; see also column 13 (emphasis in column 13, line 44 through column 14, line 31) *(US Patent 5,960,170)*. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and system of Chen et al to provide a database based on hierarchical parse tree for parsing to retrieve each suspect string as taught by **Chen**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Chen** so as to perform a more effective virus scan based on specific type of file and directory based on computer resources (column 18, lines 2-15*(US Patent 5,960,170)*).

As per claims 2 and 18, Chen et al. discloses the limitation of further comprising: the macro virus definition data files being indexed into the macro virus families categorized by a replication method employed, for example (see column 8).

As per claims 3 and 19, Chen et al. discloses the limitation of wherein the suspect string comprises part of a suspect file comprising a plurality of individual suspect strings, for example (see columns 14-15).

As per claims 4 and 20, Chen et al. discloses the limitation of further comprising: the macro virus checker identifying a replication method substantially common to a plurality of the individual suspect strings in the suspect file, for example (see column 14, lines 16 et seq.).

As per claims 5 and 21, Chen et al. discloses the limitation of further comprising: the macro virus checker identifying the macro virus family by which the common replication method is indexed, for example (see column 14, lines 16 et seq. and column 8, line 40 through column 9, line 15).

As per claims 6 and 22, Chen et al. discloses the limitation of further comprising: the macro virus definitions database storing string constants common to each macro virus family in the macro virus attributes for the macro virus definition data files, for example (see column 8, lines 6 et seq. and column 13, line 20 through column 14 and column 14, line 52 through column 15); and the macro virus checker comparing the suspect string to the string constants in the one or more macro virus definition data files for each macro virus family, for example (see column 8, lines 6 et seq. and column 13, line 20 through column 14 and column 14, line 52 through column 15).

As per claims 7 and 23, Chen et al. discloses the limitation of further comprising: a parameter specifying a threshold to matches of commonly shared string constants, for example (see column 15, lines 1-12).

As per claims 8, 24, 38, and 43, Chen et al. discloses the limitation of further comprising: a parameter specifying a minimum length of commonly shared string constants, for example (see column 15, lines 1-12).

As per claims 9 and 25, Chen et al. discloses the limitation of further comprising: the macro virus definitions database storing source code text common to each macro virus family in the macro virus attributes for the macro virus definition data files; and the macro virus checker comparing the suspect string to the source code text in the one or more macro virus definition data files for each macro virus family, for example (see column 14).

As per claims 10, 26, 37, and 42, Chen et al. discloses the limitation of further comprising: a parameter specifying a threshold to matches of commonly shared source code text, for example (see column 12, lines 3-40 and column 13, line 20 through column 14).

As per claims 11 and 27, Chen et al. discloses the limitation of further comprising: a set of keywords used in the stored source code text to identify each replication method employed, for example (see column 12, lines 3-40 and column 13, line 20 through column 14).

As per claims 14 and 30, Chen et al. discloses the limitation of further comprising: the macro virus checker parsing macro virus attributes from one or more file objects and analyzing the macro virus definition data files by index for each macro virus family, for example (see columns 12-14).

As per claims 15 and 31, Chen et al. discloses the limitation of further comprising: the macro virus checker cross referencing at least one of a string constant and source code text from the parsed macro file attributes against the macro virus attributes defined in the virus definition data files, for example (see columns 12-14).

As per claims 16 and 32, Chen et al. discloses the limitation of further comprising: the macro virus checker iteratively retrieving each macro virus definition data file using the index for each macro virus family and providing the macro virus attributes defined in the retrieved macro virus definition data file, for example (see columns 12-14).

As per claims 35 and 40, Chen et al. discloses the limitation of further comprising: each macro virus family defined according to a replication method substantially common to each of the macro virus definition data files associated with one such index, for example (see column 14, lines 16 et seq. and column 8, line 40 through column 9, line 15).

As per claims 36 and 41, Chen et al. discloses the limitation of further comprising: the macro virus definitions database storing at least one of string constants and source code text common to each macro virus family in the macro virus attributes for the macro virus definition data files, for example (see column 14, lines 16 et seq. and column 8, line 40 through column 9, line 15 and column 12, lines 3-40 and column 13, line 20 through column 14); and the macro virus checker comparing the suspect string to the at least one of the string constants and the source code text in the one or more macro virus definition data files for each macro virus family, for example (see column 14, lines 16 et seq. and column 8, line 40 through column 9, line 15 and column 12, lines 3-40 and column 13, line 20 through column 14).

As per claims 12, 13, 28, and 29, Chen et al. substantially discloses the limitation of updating information when new virus is found which includes updating the index by writing new information to corresponding set of data that meets the recitation of further comprising: the macro virus checker resetting the index referencing one or more of the macro virus definition data files for at least one macro virus family and creating a new macro virus definition data file entry comprising an index referencing one or more macro virus definition files, for example (see column 9, lines 15 see also figure 9) and discloses the new macro virus definition data file entry defining the macro virus attributes by storing at least one of a. string constant and source code text, for example (see column 9 through column 10, line 27), **Chen et al.** is silent about resetting the index referencing one or more data files because it is obvious to one skilled in the art that to add new identifier the order may need resetting. Therefore, resetting the index referencing one

or more of the macro virus definition data files for at least one macro virus family does not depart from the spirit and scope of the invention disclosed by **Chen et al.**.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

6.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Carl Colin
Patent Examiner
February 28, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100